

An Effective Dynamical Bogomolov Property

Lukas Pottmeyer

17. Januar 2012

Abstract

Let E be an Tate elliptic curve defined over a number field K with fixed non-archimedean absolute value v and let f be an associated Lattès map. In a previous paper we proved that the maximal algebraic extension of K , which is unramified at v , has the Bogomolov-Property related to the canonical height related to f (i.e. the height is either 0 or bounded from below by a positive constant). In this paper we make this bound effective and generalize the previous result to sets with bounded ramification indices over v . We also prove that an analogue result for the Néron-Tate height on E is true.

Definition 1. *Let K be a field with characteristic 0 and E an elliptic curve over K with given endomorphism $\Psi \neq [0]$. Consider a finite covering $\pi : E \rightarrow \mathbb{P}_K^1$. The map f is called Lattès map associated to E if the diagram*

$$\begin{array}{ccc} E & \xrightarrow{\Psi} & E \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}_K^1 & \xrightarrow{f} & \mathbb{P}_K^1 \end{array} \quad (1)$$

commutes. If it is necessary to be more precise, we call such a Lattès map associated to E , π and Ψ .

We talk of a Lattès map over a field K , if it is associated to an elliptic curve over K . Let E be given in (dehomogenized) Weierstrass equation, then there are the following possibilities for π (see [Si07], Proposition 6.37):

$$\pi(x, y) = \begin{cases} x & , \text{ in any case} \\ x^2 & , \text{ if } j_E = 1728 \\ x^3 & , \text{ if } j_E = 0 \\ y & , \text{ if } j_E = 0 \end{cases}$$

Although it is a well known fact, we will prove the following lemma.

Lemma 2. *Let K be a subfield of $\overline{\mathbb{Q}}$, E an elliptic curve over K and f a Lattès map associated to E with the diagram (1). Then we have*

$$\widehat{h}_f \circ \pi = \deg(\pi) \widehat{h}_E \quad ,$$

where \widehat{h}_f is the canonical height to f and \widehat{h}_E the canonical height to E .

Proof: Choose an even function $g \in \overline{K}(E)$. Then $g \circ \Psi$ is an even function of degree $\deg(g) \deg(\Psi)$ and by [Si99], Lemma 6.3, for every $P \in E$ we have

$$h \circ g(\Psi(P)) = \deg(\Psi) h \circ g(P) + O(1)$$

and therefore

$$4^{-N} \deg(g)^{-1} h \circ g(\Psi([2^N]P)) = 4^{-N} \deg(g)^{-1} \deg(\Psi) h \circ g([2^N]P) + 4^{-N} O(1) \quad .$$

Taking the limes $N \rightarrow \infty$ and use the commutativity of Ψ and $[2^N]$ we get

$$\widehat{h}_E(\Psi(P)) = \deg(\Psi) \widehat{h}_E(P) \quad . \quad (2)$$

In (1) π can be given by either $\pi(x, y) = x$ or $\pi(x, y) = x^2$ or $\pi(x, y) = x^3$ or $\pi(x, y) = y$. π is even in the first three cases, and so in these cases we have

$$\widehat{h}_f \circ \pi = \deg(\pi) \widehat{h}_E + O(1) \quad . \quad (3)$$

This follows immediately from basic properties of the canonical heights. If π is given by projection on the y -coordinate, then π^2 is even. With the trivial facts $h \circ \pi^2 = 2h \circ \pi$ and $\deg(\pi^2) = 2 \deg(\pi)$, we get that (3) holds in any case.

We combine (2) and (3) and use the fact $\deg(f) = \deg(\Psi)$ to get

$$\begin{aligned} \widehat{h}_f \circ \pi(P) &= \deg(f)^{-N} \widehat{h}_f(f^N(\pi(P))) \\ &= \deg(\Psi)^{-N} \widehat{h}_f \circ \pi(\Psi^N(P)) \\ &= \deg(\Psi)^{-N} (\deg(\pi) \widehat{h}_E(\Psi^N(P)) + O(1)) \\ &= \deg(\pi) \widehat{h}_E(P) + \deg(\Psi)^{-N} O(1) \quad \text{for all } N \in \mathbb{N} \end{aligned}$$

Taking $N \rightarrow \infty$ we get $\widehat{h}_f \circ \pi = \deg(\pi) \widehat{h}_E$. □

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field K and $\gamma \in K^*$. The elliptic curve

$$E_\gamma : y^2 = x^3 + \gamma^{-2}A + \gamma^{-3}B$$

over K is the twist of E at γ . Notice that this is a Weierstrass equation of the curve given by $\gamma y = x^3 + Ax + B$. If A , respectively B , is equal to zero, we can choose γ in

$(K^*)^{1/3}$, respectively $(K^*)^{1/2}$. E and E_γ are isomorphic over \overline{K} , and an isomorphism is given by

$$g_\gamma : E \xrightarrow{\sim} E_\gamma \quad ; \quad (x, y) \mapsto (\gamma^{-1}x, (\gamma\sqrt{\gamma})^{-1}y)$$

As g_γ is an isomorphism it commutes with multiplication by $m \in \mathbb{Z}$. This gives a simple relation between the canonical heights on E and E_γ . For any $P \in E$ we have

$$\widehat{h}_E(P) = \frac{1}{2} \lim_{n \rightarrow \infty} \frac{1}{4^n} h(x([2]^n P)) = \frac{1}{2} \lim_{n \rightarrow \infty} \frac{1}{4^n} h(\gamma x([2]^n g_\gamma(P))) = \widehat{h}_{E_\gamma}(g_\gamma(P)) \quad (4)$$

Proposition 3. *Consider the field extensions $\mathbb{Q} \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$. Let E be an elliptic curve over K and f a Lattès map related to the diagram (1). If there is a positive constant $c > 0$, such that for every elliptic curve E' over K , which is \overline{K} -isomorphic to E , $\widehat{h}_{E'}(P) \geq c$ is true for all $P \in E'(L) \setminus E'_{tors}$, then we have*

$$\widehat{h}_f(\alpha) \geq \deg(\pi)c \text{ for all } \alpha \in L \setminus \text{PrePer}(f) \quad .$$

Epecially this holds if c depends only on the j -invariant of E .

Proof: The proof goes as follows. Take an arbitrary $\alpha \in L \setminus \text{PrePer}(f)$ and a point $P \in E(\overline{K})$, with $\pi(P) = \alpha$. As α is non preperiodic we know that P is not a torsion point. Twist E at a suitable γ , such that $g_\gamma(P) \in E_\gamma(L)$ and then use Lemma 2, (4) and our assumption to conclude

$$\widehat{h}_f(\alpha) = \deg(\pi)\widehat{h}_E(P) = \deg(\pi)\widehat{h}_{E_\gamma}(g_\gamma(P)) \geq \deg(\pi)c \quad .$$

We will do this by a case by case consideration, regarding the possible representations of π .

First, let π be given as the projection on the x -coordinate. Define $\beta := \alpha^3 + A\alpha + B$. If β is a square in L , then P is in $E(L)$ and there is nothing more to prove. Let β be no square in L and fix a square root $\sqrt{\beta}$ in the algebraic closure, such that $P = (\alpha, \sqrt{\beta})$. Consider the quadratic twist of E at β . Then

$$g_\beta(P) = \left(\frac{\alpha}{\beta}, \beta^{-1}\right) \in E_\beta(L) \quad .$$

In the second case, we take $\pi(x, y) = x^2$. Notice, that this can only occur if $j_E = 1728$, so we can assume $E : y^2 = x^3 + Ax$. For fixed roots, we have $P = (\sqrt{\alpha}, \sqrt[4]{\alpha}\sqrt{\alpha+A})$. If α is in L^2 we argue exactly as in the first case. If α is no square in L , then we first twist E at $\sqrt{\alpha}$ and see that $g_{\sqrt{\alpha}}(P) = (1, \sqrt{1 + \frac{A}{\alpha}}) \in E(\overline{K})$. Like in the first case $g_{\sqrt{\alpha}}(P)$ is either in $E_{\sqrt{\alpha}}(L)$ or can be seen as an element of $(E_{\sqrt{\alpha}})_{1+\frac{A}{\alpha}}(L)$. Both yields the desired result.

The cases $\pi(x, y) = x^3$ and $\pi(x, y) = y$ are only possible if $j_E = 0$, so we have $E : y^2 = x^3 + B$. When a twist is necessary, then for $\pi(x, y) = x^3$ twist E at $\gamma_1 := \sqrt[3]{\alpha^2 - B}$ and for $\pi(x, y) = y$ twist E at $\gamma_2 := \sqrt[3]{\alpha}$ (again for fixed roots). Either yields $x(g_{\gamma_i}(P)) \in L$ and $y(g_{\gamma_i}(P)) \in L^2$. Thus we can proceed as usual like in the first case. \square

Definition 4. Let p be a rational prime and $e, f \in \mathbb{N}$. We call a subfield L of $\overline{\mathbb{Q}}$ totally p -adic of type (e, f) if for every $\alpha \in L$ and all $w \in M_{\mathbb{Q}(\alpha)}$, with $w \mid p$, the ramification indices $e_{w|p}$ are bounded by e and the residue degrees $f_{w|p}$ are bounded by f .

Example 1. Let K be a number field and $K^{(d)}$ be the compositum of all fields F with $[F : K] = d$. For a non archimedean absolute value $v \mid p$ on K there are only finitely many field extensions of K_v of degree d . See for example [Na], Corollary 2 of Theorem 5.27. So $[K(\alpha)_w : K_v]$ is uniformly bounded for all $\alpha \in K^{(d)}$ and $w \mid v$, $w \in M_{K(\alpha)}$. Especially $e_{w|p}$ and $f_{w|p}$ are uniformly bounded for all $\alpha \in K^{(d)}$. If we denote the bounds by e and f , then $K^{(d)}$ is a totally p -adic field of type (e, f) . Recently Checcoli and Widmer proved, that also $(\dots (K^{(d)})^{(d)} \dots)^{(d)}$ is totally p -adic of type (e', f') for some $e', f' \in \mathbb{N}$ (see [CW11]).

The next corollary follows immediately from Theorems of Baker and Petsche.

Corollary 5. Let \mathbb{Q}^{tr} be the maximal algebraic totally real field extension of \mathbb{Q} , μ the set of all roots of unity and f a Lattès map over \mathbb{Q}^{tr} . Then we have:

$$i) \quad \widehat{h}_f(\alpha) \geq \frac{1}{108(h(j_E)+10)^5} \text{ for all } \alpha \in \mathbb{Q}^{tr} \setminus \text{PrePer}(f)$$

$$ii) \quad |\text{PrePer}(f) \cap \mathbb{Q}^{tr}| \leq \frac{3}{2}(h(j_E) + 10)^2$$

$$iii) \quad \widehat{h}_f(\alpha) \geq \frac{1}{432(h(j_E)+10)^5} \text{ for all } \alpha \in \mathbb{Q}^{tr}(\mu) \setminus \text{PrePer}(f)$$

$$iv) \quad |\text{PrePer}(f) \cap \mathbb{Q}^{tr}(\mu)| \leq 18(h(j_E) + 10)^4$$

Now let K be a number field, p an odd prime and E an elliptic curve over K having no additive reduction at all places of K lying over p . If L/K is a totally p -adic field of type (e, f) , for $e, f \in \mathbb{N}$, and f a Lattès map associated to E then we have:

$$v) \quad \widehat{h}_f(\alpha) \geq \frac{25}{256} \left(\frac{\log p}{6eM} \right)^3 (\log(6eM) + \frac{\log p}{3e} + \frac{1}{6}h(j_E) + \frac{32}{5})^{-2} \text{ for all } \alpha \in L \setminus \text{PrePer}(f)$$

$$vi) \quad |\text{PrePer}(f) \cap L| \leq \frac{4eM'}{5 \log p} (\log(eM') + \frac{2 \log p}{e} + \frac{1}{6}h(j_E) + \frac{32}{5})$$

For $M = \max\{p^{6f} + 1 + 2p^{3f}, 72e\nu\}$ and $M' = \max\{p^f + 1 + 2\sqrt{p^f}, 12e\nu\}$, where ν is the maximum of 0 and $-\text{ord}_w(j_E)$ for all places $w \in M_K$ lying above p .

Proof: See [BP05] for the results concerning \hat{h}_E . Everything but $v)$ now follows from Proposition 3 and the fact, that the degree of π is at least 2. The reduction type of an elliptic curve over a place v is in general not preserved under \overline{K} -isomorphisms. So we can not apply Proposition 3 to prove $v)$. By the multiplicativity of the ramification index and the inertia degree, every extension of L of degree n is a p -adic field of type (ne, nf) . Let α be any non-preperiodic element in L and $P \in E(\overline{K})$ with $\pi(P) = \alpha$. Then P is defined over a p -adic field of type $(6e, 6f)$, since the degree of π is at most 6. Applying Theorem 21 in [BP05] and Lemma 2 leads us to the estimation in $v)$. \square

To the best of my knowledge, these are the only examples for non trivial Bogomolov-properties related to Lattès maps. In what follows we will prove that under the assumption of a Tate elliptic curve we can drop the necessity of the bound f in $v)$ and $vi)$ of Corollary 5.

Let K be a non-archimedean number field with absolute value $v \mid p$ and E_q a Tate elliptic curve over K with j -invariant j . By d we denote the degree $[K : \mathbb{Q}]$ and by d_v the local degree $[K_v : \mathbb{Q}_p]$. Let further f be a Lattès map related to the reduced Lattès-diagram given in (1). Here π is the projection on the x -coordinate, since $|j|_v > 1$ for every Tate curve. For a fixed $e \in \mathbb{N}$ we define

$$M_e := \{\alpha \in \overline{\mathbb{Q}} \mid e_{w|v} \leq e \text{ for all } w \in M_{K(\alpha)}, w \mid v\} \text{ and}$$

$$M_e^E := \{P \in E_q(\overline{\mathbb{Q}}) \mid e_{w|v} \leq e \text{ for all } w \in M_{K(P)}, w \mid v\},$$

where $e_{w|v}$ is the ramification index of w over v . Let further \hat{h}_f be the canonical height related to f and \hat{h}_E the Néron-Tate height on E_q . Based on an idea of Sinnou David we will proof:

Theorem 6. *There is an effective computable constant $c'(E_q, e) > 0$, only depending on E_q and e , with $\hat{h}_E(P) \geq c'(E_q, e)$ for all $P \in M_e^E \setminus \text{Tor}(E_q)$. Furthermore there are only finitely many torsion points in M_e^E . More precisely, we have*

$$i) \quad \hat{h}_E(P) \geq \frac{\frac{\log p}{2d} \mathfrak{c} - 3 \log 2}{(8\mathfrak{c}^3 - 2\mathfrak{c})(e! \text{ord}_v(q))^2} > 0 \text{ for all } P \in M_e^E \setminus \text{Tor}(E_q)$$

$$ii) \quad |\text{Tor}(E_q) \cap M_e^E| < \frac{1}{6} \mathfrak{c} \text{ord}_v(q)(e!)(\mathfrak{c} \text{ord}_v(q)(e!) + 1)(2\mathfrak{c} \text{ord}_v(q)(e!) + 1).$$

Where $\mathfrak{c} := \left\lceil \frac{10d}{\log p} \left(\log\left(\frac{6d}{\log p}\right) + \frac{1}{6}h(j) + \frac{22}{3} \right) \right\rceil$.

Once we have proven this, Proposition 3 immediately gives us

Theorem 7. *There is an effective computable constant $c(E_q, e) > 0$, only depending on E_q and e , with $\widehat{h}_f(\alpha) \geq c(E_q, e)$ for all $\alpha \in M_e \setminus \text{PrePer}(f)$. Furthermore there are only finitely many preperiodic points in M_e . With the notation of Theorem 6, we have*

$$i) \widehat{h}_f(\alpha) \geq \frac{\frac{\log p}{2d} \mathfrak{c} - 3 \log 2}{(4\mathfrak{c}^3 - \mathfrak{c})(e! \text{ord}_v(q))^2} > 0 \text{ for all } \alpha \in M_e \setminus \text{PrePer}(f)$$

$$ii) |\text{PrePer}(f) \cap M_e| < \frac{1}{12} \mathfrak{c} \text{ord}_v(q)(e!)(\mathfrak{c} \text{ord}_v(q)(e!) + 1)(2\mathfrak{c} \text{ord}_v(q)(e!) + 1).$$

Before we start the proof, we need some helpful calculations. The real Lambert- W function $W : [-\frac{1}{e}, \infty) \rightarrow \mathbb{R}$ is given as the inverse map of $F(x) = x\mathbf{e}^x$, where \mathbf{e} is the Euler constant. We have $W(-\frac{1}{e}) = -1$, but elements in $(-\frac{1}{e}, 0)$ have two pre-images under F . So, in the interval $[-\frac{1}{e}, 0)$ W has two branches. The upper branch $W_0(x)$ tends to 0 for $x \nearrow 0$ and the lower branch $W_{-1}(x)$ tends to $-\infty$ for $x \nearrow 0$. We do not need deep information on the Lambert- W function and take it mainly as an useful notation. For more information on this function we refer to [CGHJK].

Similarly as in [BP05] we will use the following lemma.

Lemma 8. *Let $a, b > 0$ be positive constants with $b \geq a$ and let $r : \mathbb{R}_+ \rightarrow \mathbb{R}$ be given by $r(x) = ax - b - \log x$. Then $r(x)$ is positive for all $x > -\frac{1}{a}W_{-1}(-a\mathbf{e}^{-b})$ and it holds the inequality*

$$\frac{5}{8} < -\frac{1}{a}W_{-1}(-a\mathbf{e}^{-b}) < \frac{8}{5a}(\log \frac{1}{a} + b) \quad .$$

Proof: $r(x)$ obviously tends to plus infinity, so we have to find the roots of $r(x)$ in order to prove the Lemma. We have

$$\begin{aligned} ax - b - \log x &= 0 \\ \Leftrightarrow \mathbf{e}^{-ax}x &= \mathbf{e}^{-b} \\ \Leftrightarrow -axe^{-ax} &= -a\mathbf{e}^{-b} \\ \Leftrightarrow x &\in \left\{ -\frac{1}{a}W_0(-a\mathbf{e}^{-b}), -\frac{1}{a}W_{-1}(-a\mathbf{e}^{-b}) \right\} \end{aligned}$$

Our assumption on b provides, that $W_0(-a\mathbf{e}^{-b})$ and $W_{-1}(-a\mathbf{e}^{-b})$ are defined. As we have $-\frac{1}{a}W_0(-a\mathbf{e}^{-b}) \leq -\frac{1}{a}W_{-1}(-a\mathbf{e}^{-b})$ we know that $r(x) \geq 0$, for all $x \geq -\frac{1}{a}W_{-1}(-a\mathbf{e}^{-b})$. This proves the first part of the Lemma. Now let y be in the interval $[-\frac{1}{e}, 0)$. By definition we have $y = W_{-1}(y)\mathbf{e}^{W_{-1}(y)}$. Multiplying this equation by -1 and taking the logarithm yields

$$\log(-y) = \log(-W_{-1}(y)) + W_{-1}(y) = W_{-1}(y) \left(1 - \frac{\log(-W_{-1}(y))}{-W_{-1}(y)} \right) \leq \frac{\mathbf{e} - 1}{\mathbf{e}} W_{-1}(y).$$

As $-W_{-1}(y) \geq 1$ this leads to the inequality

$$W_{-1}(y) \leq \log(-y) \leq \frac{\mathbf{e}-1}{\mathbf{e}} W_{-1}(y) \quad .$$

Applying this to $-\frac{1}{a}W_{-1}(-ae^{-b})$ and using $b \geq a$ gives us

$$\frac{\mathbf{e}}{(\mathbf{e}-1)a} \left(\log \frac{1}{a} + b \right) \geq -\frac{1}{a}W_{-1}(-ae^{-b}) \geq 1 - \frac{\log a}{a} \geq \frac{\mathbf{e}-1}{\mathbf{e}} \quad .$$

The estimation $\frac{\mathbf{e}}{\mathbf{e}-1} < \frac{8}{5}$ concludes the proof. \square

Proof of Theorem 6: Let P be a point in M_e^E , $w \mid v$ a valuation on $K(P)$ and k_P the residue field of $K(P)_w$. We choose a minimal Weierstrass equation for E_q over $K(P)$. Then \widetilde{E}_q is the reduction of E_q modulo w and $\widetilde{E}_{q_{ns}}$ is the set of all non-singular points in \widetilde{E}_q . We set $E_{q,0}(K(P)_w) := \{P \in E_q(K(P)_w) \mid \tilde{P} \in \widetilde{E}_{q_{ns}}(k_P)\}$. $E_{q,0}(K(P)_w)$ is a subgroup of $E_q(K(P)_w)$ of index $\text{ord}_w(q) = e_{w|v} \text{ord}_v(q)$ (see [Si99], Cor. IV.9.2). So we have $e_{w|v} \text{ord}_v(q)P \in E_{q,0}(K(P)_w)$. From the choice of P it is clear, that $Q := e! \text{ord}_v(q)P \in E_{q,0}(K(P)_w)$ for all $w \mid v$.

We take the local heights (also called Néron functions) λ_w on $E_q(K(P)_w) \setminus 0$, normalized such that we have the equation

$$\widehat{h}_E(P) = \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \in M_{K(P)}} d_w \lambda_w(P) \quad \forall P \in E_q(\overline{K}) \setminus 0 \quad .$$

For $Q \in E_{q,0}(K(P)_w)$ and $w \mid v$, $w \in M_{K(Q)}$, we have

$$\lambda_w(Q) = \frac{1}{2} \max\{w(x(Q)), 0\} + \frac{1}{12} w(\Delta) \geq \frac{1}{12} v(\Delta) = \frac{1}{12} v(j^{-1}) \quad . \quad (5)$$

See [Si99], Theorem VI.4.1. As we have a Tate curve, we know $v(\Delta) = v(q) = v(j^{-1}) > 0$.

We define the set $\Lambda_s = \{iQ \mid i \in \mathbb{N}, i \leq s\}$, for all $s \in \mathbb{N}$, such that Λ_s consists of pairwise distinct points. Now we will estimate $\widehat{h}_E(P)$, respectively $\widehat{h}_E(Q)$, using bounds for the local heights. For a given value w , we set w^+ to be the maximum of w and 0.

If w is archimedean, then we can use a theorem of Elkies improved by Hindry and Silverman. Namely

$$\sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \lambda_w(R - R') \geq -\frac{s}{2} \log s - \frac{11}{3} s - \frac{1}{12} w^+(j^{-1}) s. \quad (6)$$

See [HiSi90], Proposition 1.1 and [Hr87].

For a non-archimedean $w \in M_{K(P)}$ with $w(j^{-1}) \leq 0$, E_q has potential good reduction at w (See for example [Hu], Ch.5 Theorem 7.6). Let $K' \mid K(P)$ be a finite extension, such that E_q over K' has good reduction at a $w' \mid w$. Then the equation we have used in (5) shows that $\lambda_{w'}$ is not negative on $E_q(K'_{w'})$. As $\lambda_{w'}$ and λ_w coincide on $E_q(K(P)_w)$, λ_w is a non negative function.

For non archimedean absolute values w with $w(j^{-1}) > 0$ [HiSi90], Proposition 1.2 gives the inequality

$$\sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \lambda_w(R - R') \geq \frac{1}{12} \left(\frac{s}{\text{ord}_w(j^{-1})} \right)^2 w(j^{-1}) - \frac{s}{12} w(j^{-1}).$$

Thus for an arbitrary non archimedean absolute value we will use the estimation

$$\sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \lambda_w(R - R') \geq -\frac{s}{12} w^+(j^{-1}). \quad (7)$$

With (5), (6), (7) we get:

$$\begin{aligned} \sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \widehat{h}_E(R - R') &= \sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \in M_{K(P)}} d_w \lambda_w(R - R') \\ &\geq \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \mid \infty} d_w \left(-\frac{1}{2} s \log s - \frac{11}{3} s \right) - \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \mid \infty} d_w w^+(j^{-1}) \frac{1}{12} s \quad (\text{with (6)}) \\ &\quad - \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \nmid \infty, w \nmid v} d_w \frac{s}{12} w^+(j^{-1}) \quad (\text{with (7)}) \\ &\quad + \sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \mid v} d_w \frac{1}{12} v(j^{-1}) \quad (\text{with (5)}) \\ &= -\frac{1}{2} s \log s - \frac{11}{3} s - \frac{1}{[K(P) : \mathbb{Q}]} \sum_{w \nmid v} (d_w w^+(j^{-1})) \frac{s}{12} + \frac{s^2 - s}{[K(P) : \mathbb{Q}]} \sum_{w \mid v} d_w \frac{1}{12} v(j^{-1}) \end{aligned}$$

We know that for all $w \mid v$ we have $v(j^{-1}) = w(j^{-1}) = w^+(j^{-1})$. Thus we can use the definition of the standard logarithmic height h to obtain

$$\begin{aligned} \sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \widehat{h}_E(R - R') &\geq \frac{d_v v(j^{-1})}{12d} s^2 - \left(\frac{1}{12} h(j) + \frac{11}{3} \right) s - \frac{1}{2} s \log s \\ &\geq \frac{\log p}{12d} s^2 - \left(\frac{1}{12} h(j) + \frac{11}{3} \right) s - \frac{1}{2} s \log s. \end{aligned} \quad (8)$$

If P is a torsion point, then the left hand side is equal to zero. $h(j)$ is clearly greater or equal to $\frac{d_v v(j^{-1})}{d} \geq \frac{\log p}{d}$, so we can apply Lemma 8 to deduce, that the right hand side is greater zero for $s \geq \frac{48d}{5 \log p} \left(\log\left(\frac{6d}{\log p}\right) + \frac{1}{6}h(j) + \frac{22}{3} \right)$. As s is a natural number, we get a contradiction for $s = \mathfrak{c}$. This shows that there cannot exist a torsion point $P \in M_e^E$, such that the order of $e! \operatorname{ord}_v(q)P$ is greater or equal to \mathfrak{c} . Hence, there cannot exist a torsion point $P \in M_e^E$ of order greater or equal to $\mathfrak{c} \operatorname{ord}_v(q)(e!)$. Using $|E_q[k]| = k^2$ for all $k \in \mathbb{N}$, we get that there are less than $\frac{1}{6}\mathfrak{c} \operatorname{ord}_v(q)(e!)(\mathfrak{c} \operatorname{ord}_v(q)(e!) + 1)(2\mathfrak{c} \operatorname{ord}_v(q)(e!) + 1)$ torsion points in M_e^E . From now on we assume, that P is no torsion point. Then Λ_s is defined for all $s \in \mathbb{N}$, and so (8) holds for all $s \in \mathbb{N}$. The definition of Λ_s and the property $\widehat{h}_E(kQ) = k^2 \widehat{h}_E(Q)$ for all $k \in \mathbb{Z}$, leads us to

$$\sum_{\substack{R, R' \in \Lambda_s \\ R \neq R'}} \widehat{h}_E(R - R') = \left(2 \sum_{i=1}^{s-1} i^2 (s - i) \right) \widehat{h}_E(Q) = \left(\frac{1}{6}s^4 - \frac{1}{6}s^2 \right) \widehat{h}_E(Q). \quad (9)$$

If we further use (8) and the definition of Q we find that the height $\widehat{h}_E(P)$ is bounded from below by

$$c'(E_q, e) := \max_{s \in \mathbb{N}} \frac{\frac{\log p}{2d}s - \left(\frac{1}{2}h(j) + 22\right) - 3 \log s}{(s^3 - s)(e! \operatorname{ord}_v(q))^2}.$$

$c'(E_q, e)$ is obviously positive. In what follows we will give a lower bound for $c'(E_q, e)$. Let $\mathfrak{c}_W := -\frac{6d}{\log p} W_{-1} \left(-\frac{\log p}{6d} H(j)^{1/6} \mathbf{e}^{22/3} \right)$ be the greatest root of the real function $r(x) = \frac{\log p}{2d}x - \left(\frac{1}{2}h(j) + 22\right) - 3 \log x$ (see Lemma 8). Then we know that this function is strictly positive for all $x > \mathfrak{c}_W$. Especially we have $r(2x) \geq \frac{\log p}{2d}x - 3 \log 2$, for all $x \geq \mathfrak{c}_W$, with equality if and only if $x = \mathfrak{c}_W$. By Lemma 8 (again) we have $1 < 2\mathfrak{c}_W < 2\mathfrak{c}$. With this we finally deduce

$$c'(E_q, e) \geq \frac{r(2\mathfrak{c})}{(8\mathfrak{c}^3 - 2\mathfrak{c})(e! \operatorname{ord}_v(q))^2} \geq \frac{\frac{\log p}{2d}\mathfrak{c} - 3 \log 2}{(8\mathfrak{c}^3 - 2\mathfrak{c})(e! \operatorname{ord}_v(q))^2} > 0,$$

what concludes the proof. \square

Remark 1. In both theorems we can get slightly better bounds, if we set $\mathfrak{c} := \left\lceil -\frac{6d}{\log p} W_{-1} \left(-\frac{\log p}{6d} H(j)^{1/6} \mathbf{e}^{22/3} \right) \right\rceil$, where $H(j)$ denotes the multiplicative height of j . Notice, that W_{-1} can be easily computed with Maple.

We have proven a lower bound for the canonical heights \widehat{h}_E and \widehat{h}_f on sets. Our main interest concerns lower bounds on fields. If we assume L to be a field, such

that L is a subset of M_e for some e , Theorem 6 and Theorem 7 give us a lower bound for the canonical heights on $E_q(L) \setminus \text{Tor}(E_q)$, respectively $L \setminus \text{PrePer}(f)$. But we can achieve much nicer bounds if we additionally assume that L/K is normal. In this case, the term $e!$ in our bound can be replaced by e . Formally:

Corollary 9. *Let K , v , E_q and \mathfrak{c} be as in theorem 6. Let further L/K be a galois extension with $L \subset M_e$ for a fixed $e \in \mathbb{N}$. Then we have*

- i) $\widehat{h}_E(P) \geq \frac{\frac{\log p}{2d} \mathfrak{c} - 3 \log 2}{(8\mathfrak{c}^3 - 2\mathfrak{c})(e \text{ord}_v(q))^2} > 0$ for all $P \in E_q(L) \setminus \text{Tor}(E_q)$
- ii) $|\text{Tor}(E_q) \cap M_e^E| < \frac{1}{6} \mathfrak{c} \text{ord}_v(q) e (\mathfrak{c} \text{ord}_v(q) e + 1) (2\mathfrak{c} \text{ord}_v(q) e + 1)$.

Proof: In the proof of theorem 6, $e!$ was an estimation for the lowest common multiple of all $e_{w|v}$, $w \in M_{K(P)}$, which does not depend on P . Now let $K'(P)$ be the normal closure of $K(P)$. From our assumption we know, that $K'(P)$ is contained in $L \subset M_e$. Thus we have $e_{w'|v} \leq e$ for all $w' \in M_{K'(P)}$ lying above v . Exactly like in the proof of theorem 6 we conclude, that for all these w' we have $e_{w'|v} \text{ord}_v(q)P \in E_{q,0}(K'(P)_{w'})$. But as $K'(P)/K$ is galois, we know that all these $e_{w'|v} =: e_v$ are equal. Hence, we set $Q := e_v \text{ord}_v(q)P$, where $e_v \leq e$, and proceed with the proof as before. Notice again, that for every $w \in M_{K(P)}$ there is a $w' \in M_{K'(P)}$ such that $\lambda_w(Q) = \lambda_{w'}(Q)$. \square

By Proposition 3, the analogue result for \widehat{h}_f holds, too.

Example 2. Let $K^{nr,v}$ be the maximal algebraic extension of the number field K , which is unramified at v . As sets we have $K^{nr,v} = M_1$. Then we have seen, that $K^{nr,v}$ has the Bogomolov-Property related to \widehat{h}_f , where f is a Lattès map over K related to a Tate curve. Obviously this holds for finite extensions of $K^{nr,v}$.

Example 3. Again let K be a number field with non-archimedean absolute value $v \mid p$. As a last example of a field lying inside some M_e , we will construct a field that is neither a finite extension of $K^{nr,v}$ nor a totally p -adic field of type (e, f) . This can be done by a combination of the previous two examples. Take $K^{(d)}$ as in Example 1. Fix an extension $v_d \mid v$ on $K^{(d)}$ and construct $(K^{(d)})^{nr,v_d}$, the maximal algebraic extension, that is unramified at v_d . For an arbitrary $\alpha \in (K^{(d)})^{nr,v_d}$ we have $K(\alpha) = LM$, with L a subfield of $K^{(d)}$ and $K(\alpha)/L$ is unramified at $w = v_d|_M$. Let v' be any absolute value on $K(\alpha)$, with $v' \mid w$. Then we have $e_{v'|v} = e_{v'|w} e_{w|v} = e_{w|v}$. This is uniformly bounded as L is totally p -adic of type (e, f) .

Remark 2. In general both theorems do not hold, if we start with an elliptic curve with (potentially) good reduction at v (see [Po11]). Furthermore $K^{nr,v}$ does not have the Bogomolov property related to the standard logarithmic height h . It is not hard to see, that the discriminant of $\mathbb{Q}(2^{1/2^n})$ is a power of 2. Hence, the elements $\{2^{1/2^n}\}_{n \in \mathbb{N}}$ are unramified over all odd primes and their heights clearly become arbitrary small. To deal with the prime two, it suffices to see that the discriminant of $\mathbb{Q}(5^{1/3^n})$ is odd for all $n \in \mathbb{N}$. By a comment of Philipp Habegger, another way to see that the theorems do not hold for h , is that h is defined on $\mathbb{G}_m(K^{nr,v})$. But \mathbb{G}_m has everywhere good reduction, so one can use an analogue to the first statement of this remark.

References

- [BP05] Baker, M.; Petsche, C.: *Global discrepancy and small points on elliptic curves*, International Mathematics Research Notices No. 61, 3791-3834; Oxford University Press (2005)
- [CGHJK] Corless, R.; Gonnet, G.; Hare, D.; Jeffrey, D.; Knuth, D.: *On the Lambert W Function*, Advances in Computational Mathematics, Vol. 5, 329-359; Springer (1996)
- [CW11] Checcoli, S.; Widmer, M.: *On the Northcott property and other properties related to polynomial mappings*, arXiv:1111.5060v1; (2011)
- [HiSi90] Hindry, M.; Silverman, J. H.: *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988-1989, Progr. Math., No. 91, 103-116, Birkhäuser (1990)
- [Hr87] Hriljac, P.: *Splitting fields of principal homogeneous spaces*, 1984-1985 Number Theory Seminar, Lecture Notes in Mathematics Vol. 1240, 214-229, (1987)
- [Hu] Husemöller, D.: *Elliptic Curves. Graduate Texts in Mathematics Vol.111* Second Edition; Springer (2000)
- [Na] Narkiewicz, W.: *Elementary and Analytic Theory of Algebraic Numbers*, Second Edition; PWN-Polish Scientific Publishers and Springer-Verlag (1990)

- [Po11] Pottmeyer, L.: *A Dynamical Bogomolov Property*, arXiv:1103.1294; (2011)
- [Si07] Silverman, J. H.: *The Arithmetic of Dynamical Systems. Graduate Texts in Mathematics Vol.151* ; Springer (2007)
- [Si99] Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics* ; Springer (1999)

Lukas Pottmeyer, Fakultät für Mathematik, Universität Regensburg, D-93053 Regensburg,
`lukas.pottmeyer@mathematik.uni-regensburg.de`